Compliance Component

DEFINITION

Name	System Security Certification and Accreditation Process
Description	Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The security certification requirements specific to a system will be provided by the entity requiring the certification such as the Federal Government or grantors. The certification itself is generally performed by a third party or as directed by the requesting authority. System Accreditation is the final step in the process to protect information technology systems. By accrediting an information system, an agency officially accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the agency if a breach of security occurs.
Rationale	To document that the system has the required degree of protection for confidentiality, integrity or availability as set forth by an agency or regulating body.
Benefits	• System Certification demonstrates that the security safeguards are adequate and appropriate for the system or application • System Accreditation provides the approving official with a clear understanding of a system's security readiness or a list of any deficiencies discovered • Promotes more consistent, comparable, and repeatable assessments of security controls in information systems

ASSOCIATED ARCHITECTURE LEVELS

List the Domain Name	Security
List the Discipline Name	Management Controls
List the Technology Area Name	System Security Certification and Accreditation
List Product Component Name	

COMPLIANCE COMPONENT TYPE

Document the Compliance Component Type	Guideline

Component Sub-type			
COMPLIANCE DETAIL			
State the Guideline, Standard or Legislation	The following are generally required for the certification and accreditation process: • Periodic assessments of risk in accordance with policies and procedures that ensure information security is addressed throughout the life cycle of each information system • Plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate • Security awareness training to inform system users of the information security risks associated with their activities and their responsibilities in complying with agency policies and procedures • Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls as set forth by the requesting authority • A process to address any deficiencies in the information security policies, procedures, and practices of the agency • Procedures for detecting, reporting, and responding to security incidents • Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency		
Document Source Reference #			
Standard Organization			
Name	NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems, NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems	*Website*	www.csrc.nist.gov/publications/nistpubs
Contact Information			
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		

KEYWORDS			
List all Keywords	Assessment, procedure, deficiency, practice, plan, audit, policy		
COMPONENT CLASSIFICATION			
Provide the Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Rationale for Component Classification			
Document the Rationale for Component Classification			
Conditional Use Restrictions			
Document the Conditional Use Restrictions			
Migration Strategy			
Document the Migration Strategy			
Impact Position Statement			
Document the Position Statement on Impact			
CURRENT STATUS			
Provide the Current Status)	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	09/27/07	*Date Accepted / Rejected*	10/16/07
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			